Guide to Decoding Disinformation.

Step-by-step guide to identify the main components of disinformation attacks targeting journalists and news outlets

Quick Guide

Here are four key steps that journalists, researchers, and others investigating disinformation campaigns against the media should take:

1. **Understand the context**
2. **Analyze the timeline, platform, and dissemination methods**
3. **Identify the actors involved**
4. **Pinpoint the narratives**

This document is a step-by-step guide for journalists and researchers investigating disinformation and smear campaigns against the media. It offers a framework for identifying the tactics, techniques, and procedures (TTPs) behind disinformation campaigns. In doing so, it aims to support efforts to expose and counter such campaigns, which are increasingly used to target critical media and undermine audience trust in fact-based news.

These guidelines are not **one-size-fits-all** as disinformation keeps evolving with new technologies. This is a **living document** which will be updated as new methodologies are developed.

1 Understand the context

The aim here is to understand whether and how disinformation attacks on the media reflect broader strategies to undermine public trust or advance specific narratives. These are the main elements we normally try to identify:

Relevant events and statements within the time period of the attack

Identify the broader background developments or events that have contributed to an environment in which journalists are targeted for their reporting. These could be elections, protest movements or social crises or challenges (e.g., immigration, social issues).

Identify the specific topic or public discussion that appears to have triggered the attack.

Identify statements by politicians, influential public figures or other political actors[1] that have created an environment that legitimizes attacks against journalists.

Relevant political and social context

Identify the agendas of the political or other relevant actors related to the disinformation campaign.

Media outlets and social media channels that tend to disseminate false narratives

Look at online platforms, as well as relevant mainstream media and fringe or “alternative” media.

1 Political actors: persons directly involved in party politics or governance, including: elected or appointed officials, holding political positions in any branch or level of government; persons active in political parties. Other relevant actors: public figures not directly involved in politics, but engaged in public discourse on policy-related topics.

2 Analyze the timeline, platform, and dissemination methods

Researchers and journalists should develop a timeline of the attack to better understand the flow of the disinformation campaign. Additionally, you should identify the platforms used to deploy the campaign, as well as the vectors used to enhance its dissemination, such as hashtags, memes and AI-generated video/audio deepfakes.

Develop a timeline of the attack: Identify and describe the key event(s) related to the attacks and create a timeline

First and foremost, interview the target of the campaign to get an initial account of the attack. Targeted journalists often have a good understanding of the most important components of disinformation campaigns and can provide invaluable context, helping to draw an initial timeline of the campaign. If the target was a media organization, talk to relevant staff members: editors, journalists, community managers or digital security experts.

Note the journalistic piece of work that was used to ignite the smear campaign against the journalist or news outlet.

Note when and where (platforms, websites, etc.) the first instances of the attacks were identified and list them chronologically. In doing so, describe how the campaign was deployed across platforms through the period of time that the attack lasted.

Some outlets keep continuous records of attacks and harassment, so make sure to check them and include any instances linked to the attack under investigation.

Identify the channels of attacks and harassment

Search social media for pages and profiles mentioning the target: Telegram, X, YouTube and Facebook are most common (as of 2024), but also look into Instagram, Threads, Reddit, TikTok, WhatsApp and other platforms depending on their popularity in the local context.

Attacks and harassment are often carried out through “fringe” media outlets, and websites impersonating media outlets (See section 3). In cases where the background of these platforms is not clear, use available data (official registries, impressum data), to try to determine ownership and editorial background.

Identify what elements have been used to more quickly disseminate the smear campaign

Search for hashtags, memes, altered pictures, videos, slurs, personal information, video/audio deepfakes across different platforms. Bear in mind that not every single posting is in itself a clear threat, so record also instances of veiled threats or other intimidation techniques such as doxxing (some part of personal information has been exposed, normally the email or phone number of the targeted journalist) to get a whole picture of the narratives.

Note if there are SLAPP suits or threats of lawsuits connected with the attacks.

Note if the journalist or news outlet has been recently targeted with cyberattacks.

Identify press releases, official statements and media appearances of relevant political or other actors.

BEST PRACTICE

Archive URLs with all instances of attacks or false narratives directed at the target

You can create internal system of archiving or use platforms such as ghostarchive.org or archive.org

3 Identify the actors involved

For the purpose of the investigation, it is important to identify those actors who have instigated and / or triggered the attack and those who have, in fact, carried it out. These actors can be political, chat groups, pages, anonymous profiles, fringe media, and any other relevant actors linked to the disinformation campaign.

Identify and describe the most influential actors that have instigated the disinformation campaign

- Note short bio, political or other affiliation, social media accounts and followings, relevant statements for every identified political actor.
- Look for those instances in which these actors called on their followers to target the journalist or the news outlet.

Identify and describe most relevant (fringe[2]) media actors that were favorably reporting on the attack and supporting disinfo narratives

- Check the details of the website owner and the site's compliance with national laws.
- Note presence on social media including followers.
- Check Internet Archive (Wayback Machine) for previous iterations of the website. This might reveal "about" pages that were active in the past but subsequently removed by administrators.
- Check media databases such as Newsguard for more insight.

2 We consider fringe media to be those internet sites that present themselves as media, but operate outside the so-called media mainstream, and often do not adhere to professional journalistic standards in their work. They are often non-transparent in terms of ownership and editorial structure, the contributions they publish are often unsigned, and they regularly publish manipulative and misinformation content. The purpose of their work is not to exercise the public's right to access information of public interest, but to monetise sensationalist content and/or promote the agenda of certain interest groups.

BEST PRACTICE

Perform an infrastructure analysis of the main actors involved as well as the websites. This analysis might require teaming up with IT personnel or OSINT experts and can include, among other:

- DNS analysis of the propaganda sites
- Reverse Image Searching of logos, icons or images to trace them back to other publications
- Domain and IP lookup

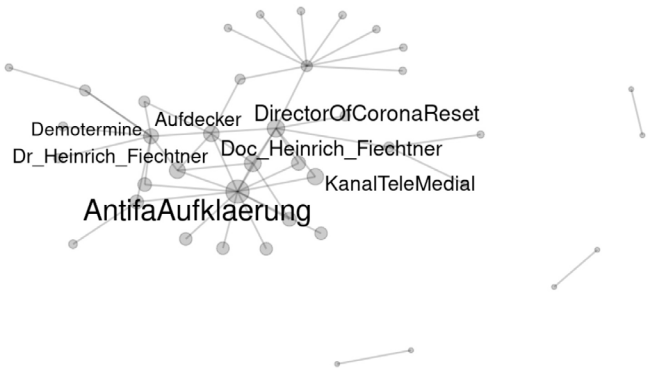
BEST PRACTICE

Perform a social network analysis to discover linkages and actors and how they are connected

A number of professional tools and companies can conduct this kind of analysis, adjusted to your needs. These are helpful in identifying actors missed during the basic search and can show the spread of messages connected to attacks. Here is a list of software we have worked with:

- Gephi - The Open Graph Viz Platform
- NodeXL
- Gerulata
- Kivu.tech

Example: Learn more about the network of channels in Telegram that were sharing intimidating messages against a local journalist in Germany.



Click here to read the full report.

4 Pinpoint the narratives

Identifying the specific narrative being spread by the disinformation attack can help reveal the purpose behind the campaign.

Fact-check the claims made during attacks

Identify and fact-check false information used in the attack about a media outlet and its political affiliation, funding, or other organizational information.

Be aware that disinformation campaigns sometimes refer to previous works of the journalists that are not strictly related to the original journalistic work that was used to ignite the smear campaign.

Identification of the disinformation narratives

Do a content analysis of social media publications and media articles and of public speeches.

Note the wording and phrases used, pay attention to neologisms.

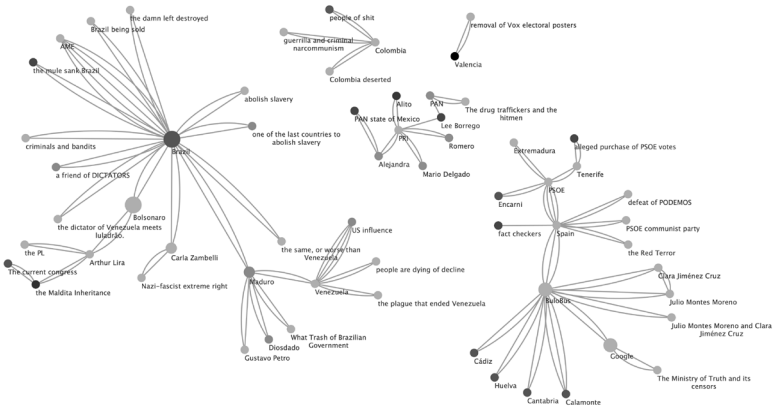
Use the catalog of disinformation narratives available on the European Digital Media Observatory (EDMO) page (in Europe) and connect your findings with existing disinformation narratives.

BEST PRACTICE

Create narrative networks and track these false narratives across time. This type of analysis offers an overview of how narratives against journalists are connected and disseminated in the same channels and at the same time, giving you a comprehensive understanding of the broader rhetoric

Most of the tools that are able to perform narrative networks rely on AI. In this case, please make sure that you follow transparency principles on the use of AI technology in the newsroom. There are several guidelines but you can start with Partnership on AI's principles that you can find here.

Example: Learn more about the narrative networks of the conspiracy theories disseminated across Telegram channels in Spain.



Click here to read the full report.

BEST PRACTICE

Create a report on this investigation. By following these guidelines you'll be able to identify the main components that constitute a disinformation campaign and give an answer to the main journalistic questions: What? Who? Why? How? When? Where?

Distribute the report to relevant national and international stakeholders such as journalistic associations.

Before doing so, consider any legal risks (e.g. talk to journalistic associations for legal counseling or to the legal department of your news outlet). Since reports would likely name those identified as being behind attacks, is there a chance that individuals or companies could sue for defamation?

Other resources

Amnesty International: Citizen Evidence Lab

"This online space aims to support human rights organisations, researchers, investigators, students, journalists and others to explore and share digital investigative methods for human rights research."
Visit the page here.

Bellingcat's Online Investigation Toolkit

"This online open-source investigation toolkit includes guidance on satellite and mapping services, tools for verifying photos and videos, websites to archive web pages, and much more."
Visit their materials here.

Digital Forensic Research Lab

"The program consists of workshops and practical training sessions covering media literacy, open-source investigative techniques, fact-checking and source verification, narrative analysis, social media monitoring, geolocation, and many other topics."
Visit their resources & materials here.

European Digital Media Observatory (EDMO): Trainings

"EDMO offers regular online training modules aimed at supporting different stakeholders in understanding and tackling online disinformation."
Visit their training programme here.

Tactical Tech: Exposing the Invisible

"Exposing the Invisible looks at different techniques, tools and methods along with the individual practices of those working at the new frontiers of investigation."
Visit the page here.

Verification Handbook for Disinformation and Media Manipulation, by Craig Silverman

"This book equips journalists with the knowledge to investigate social media accounts, bots, private messaging apps, information operations, deep fakes, as well as other forms of disinformation and media manipulation."
Download the handbook here.

The project

Decoding the disinformation playbook of populism in Europe

IPI, Taz, and Faktograf are working together to decode populist propaganda in Europe targeting fact-checkers and investigative journalists – who are both essential players in the fight against disinformation.

*The project **Decoding the disinformation playbook of populism in Europe** is supported by the European Media and Information Fund, managed by the Calouste Gulbenkian Foundation.*

Guide developed by Tajana Broz (Faktograf) and Javier Luque Martínez (IPI).